# 实验四 ICMP 协议和IP 数据报分片分析

## 【实验目的】

1. 理解 ICMP 协议报文类型和格式；

2. 理解 ping 命令的工作原理；

3. 理解 traceroute 的工作原理；

4. 理解 IP 协议报文类型和格式。

## 【实验环境】

与因特网连接的计算机，操作系统为Windows，安装有Wireshark、IE 等软件。

## 【实验内容】

1. 使用 wireshark 抓包软件分析ICMP 协议报文的类型；

2. 分析 ping 命令的工作原理；

3. 分析 tracert 命令的工作原理；

4. 使用 wireshark 抓包软件分析IP 协议报文以及报文分片。

## 【实验步骤】

**1. 分析 ICMP 协议**

步骤1：在 PC1 运行 Wireshark，开始截获报文，为了只截获和实验内容有关的报文，将

Wireshark 的 Captrue Filter 设置为“No Broadcast and no Multicast”；

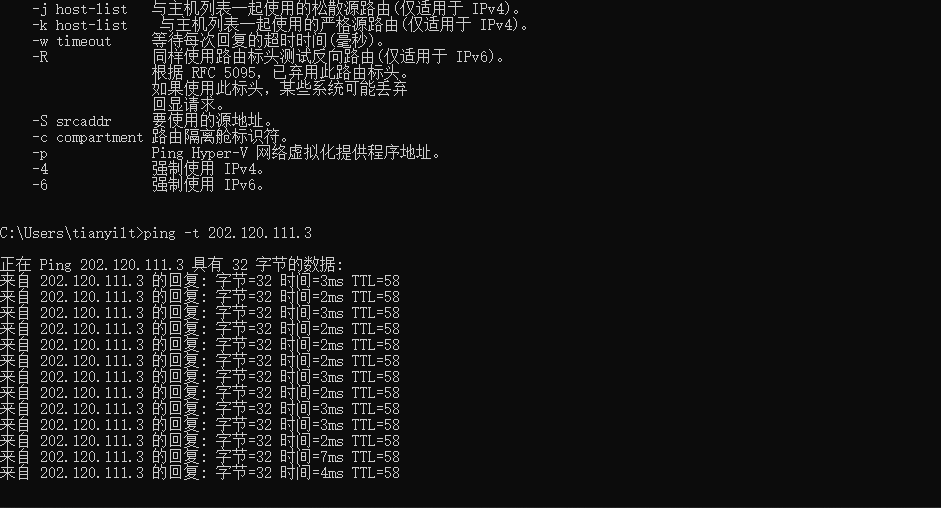
步骤2：在 PC1 以 202.120.111.3 为目标主机，在命令行窗口执行 Ping 命令，要求ping

通8 次；

**【答**】：Ping 命令为：ping 202.120.111.3

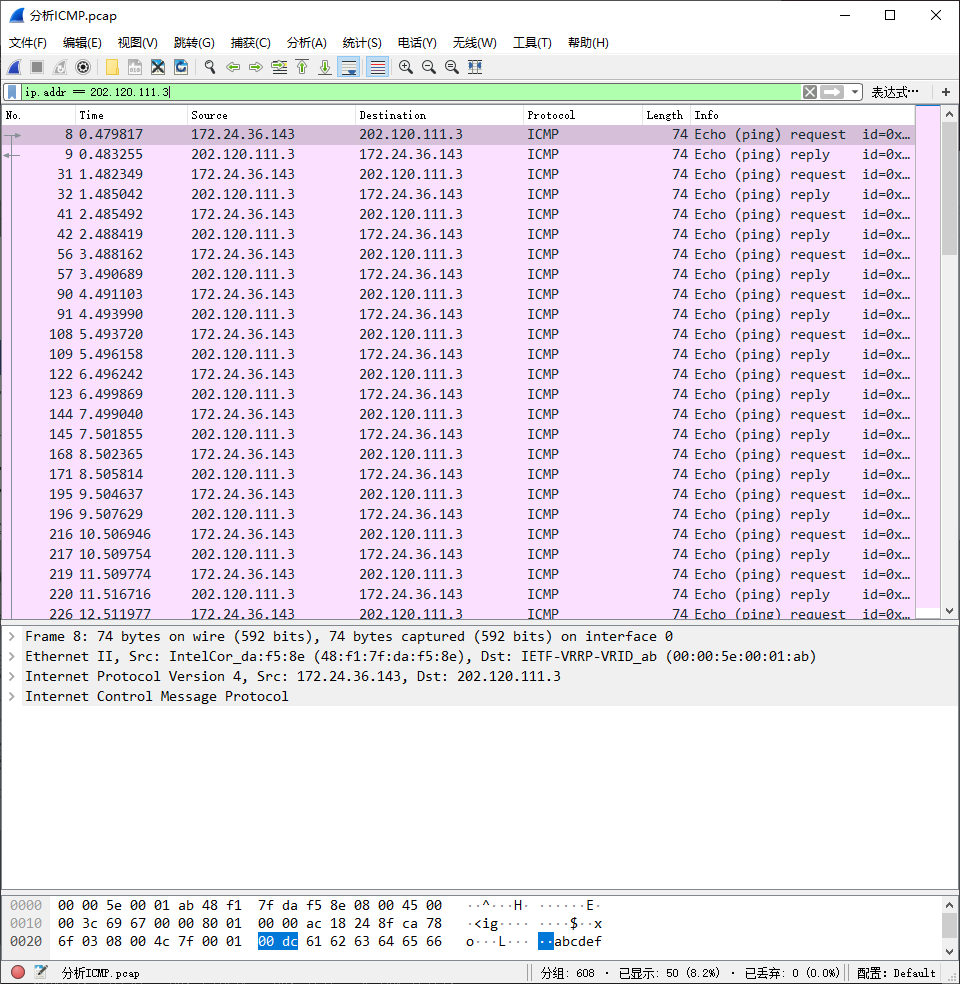
将命令行窗口进行截图：

**【答**】：



步骤3：停止截获报文，分析截获的结果，回答下列问题：

1. 将抓包结果进行截图（要求只显示 ping 的数据包）：



1. 截获的 ICMP 报文有几种类型？分别是：

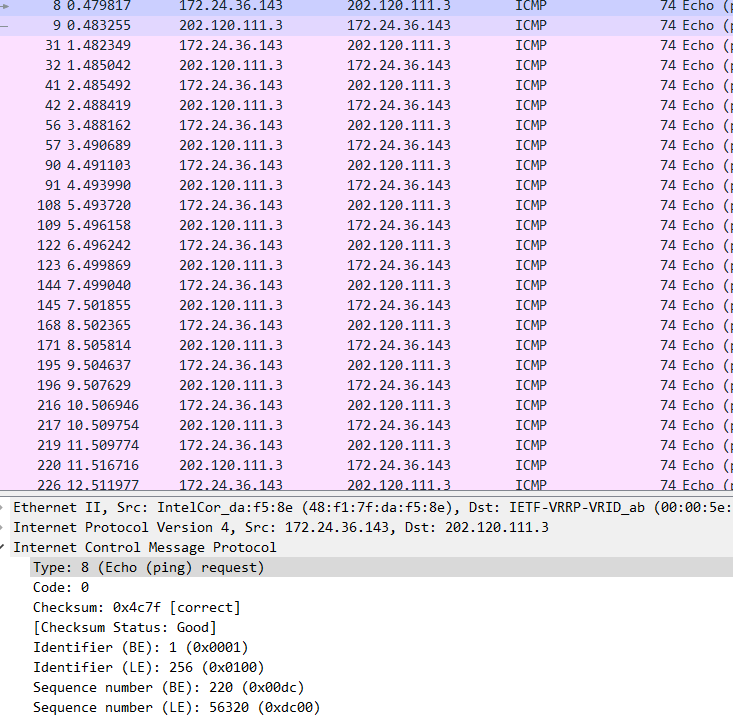
**【答**】：2种 8request 0reply

（3）分析截获的 ICMP 报文，按下表要求，将各字段信息填入表中，要求填写前4 个报文的信息。

**【答**】：

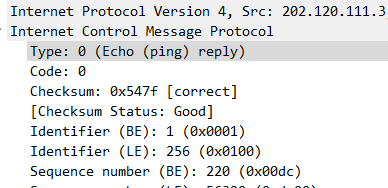
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文号** | **源IP** | **目的IP** | **报文格式** | | | | | |
| **类型** | **代码** | **标识** | | **序列号** | |
| **BE** | **LE** | **BE** | **LE** |
| 8 | 172.24.36.143 | 202.120.111.3 | Type: 8 (Echo (ping) request) | 0 | 1 | 256 | 220 | 56320 |
| 9 | 202.120.111.3 | 172.24.36.143 | Type: 0 (Echo (ping) reply) | 0 | 1 | 256 | 220 | 56320 |
| 31 | 172.24.36.143 | 202.120.111.3 | Type: 8 (Echo (ping) request) | 0 | 1 | 256 | 221 | 56576 |
| 32 | 202.120.111.3 | 172.24.36.143 | Type: 0 (Echo (ping) reply) | 0 | 1 | 256 | 221 | 56576 |

1. 查看ping 请求信息，ICMP 的type是 8。和code是 0。并截图。



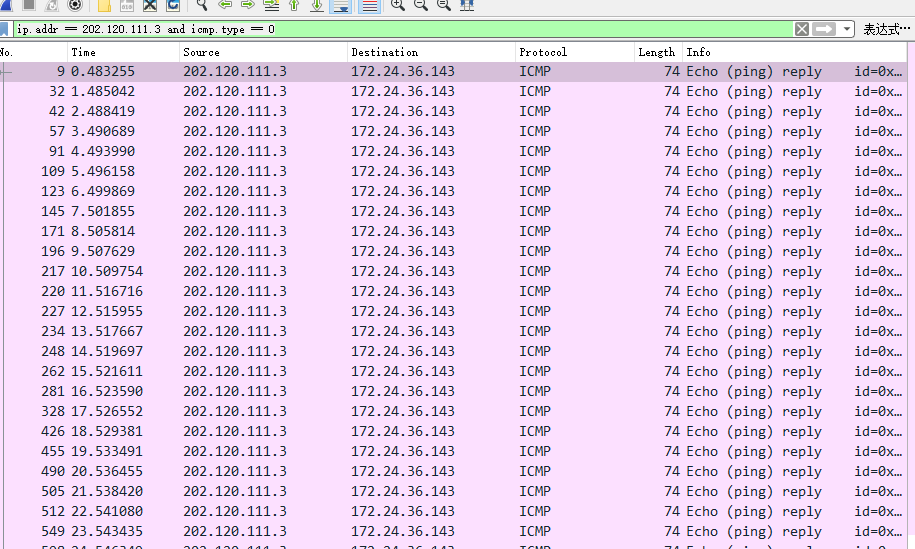
**【答**】：

1. 查看相应得ICMP 响应信息，ICMP 的type 是0\_和code 是 \_\_\_0\_。并截图。



**【答**】：

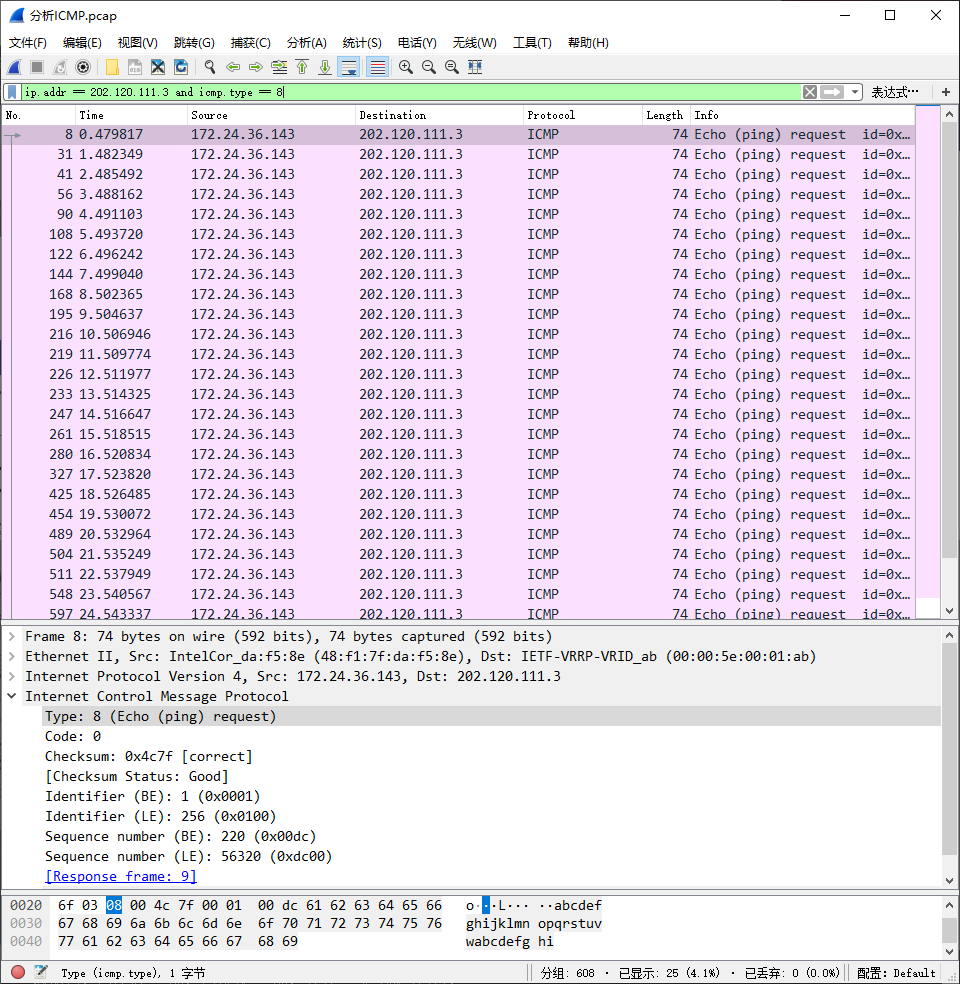
1. 若要只显示ICMP的echo响应数据包，显示过滤器的规则为ip.addr == 202.120.111.3 and icmp.type == 0.并根据过滤规则进行抓包截图。



**【答**】：

7) 若要只显示ICMP的echo请求数据包，显示过滤器的规则为ip.addr == 202.120.111.3 and icmp.type == 8. 并根据过滤规则进行抓包截图。

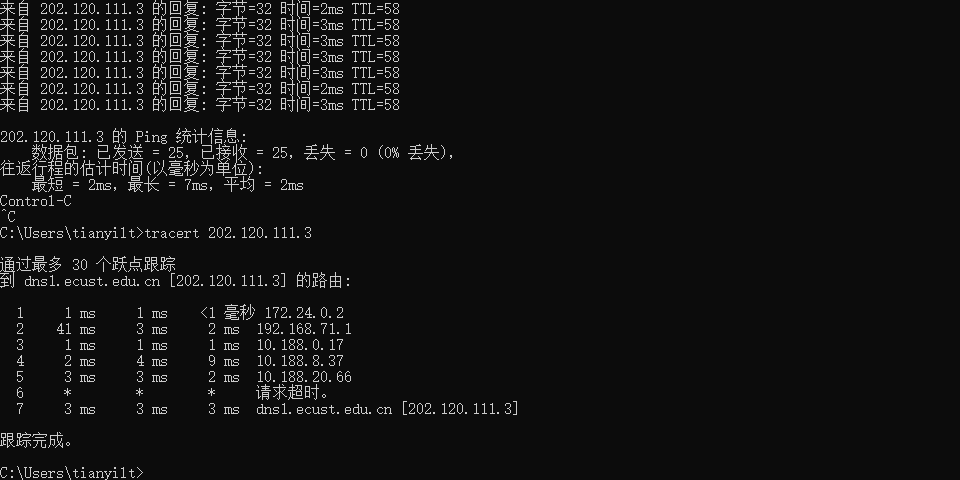
**【答**】：



**2. 分析traceroute 的工作原理**

步骤1：在 PC1 上运行 Wireshark 开始截获报文；

步骤2：在PC1上执行Tracert命令，如：tracert 202.120.111.3；将命令窗口进行截图；



步骤3：在wireshark里设置显示过滤器为icmp；

步骤4：停止截获报文，分析截获的报文，回答下列问题：

（1）截获了报文中哪几种 ICMP 报文？其类型码和代码各为多少？

**【答**】：3种

|  |  |  |
| --- | --- | --- |
| **ICMP 报文** | **类型码** | **代码** |
| 28 | 8 | 0 |
| 134 | 11 | 0 |
| 732 | 0 | 0 |

（2）在截获的报文中，哪些是超时报告报文，请截图显示所有超时报文并指出超时报告报文的源地址分别是多少？

ip.addr == 202.120.111.3 and icmp.type == 11过滤出的报文

后面的ip地址

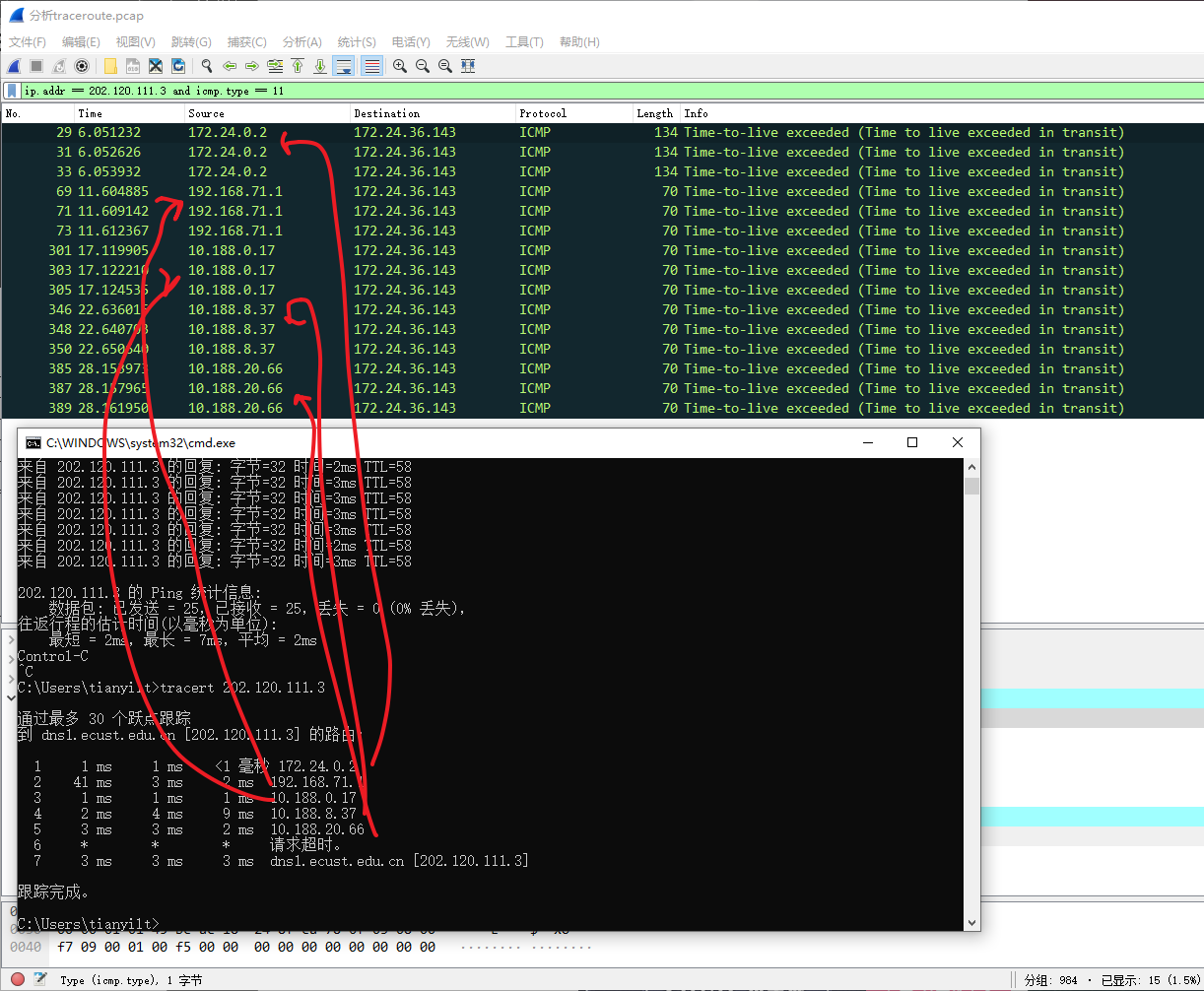
1 1 ms 1 ms <1 毫秒 172.24.0.2

2 41 ms 3 ms 2 ms 192.168.71.1

3 1 ms 1 ms 1 ms 10.188.0.17

4 2 ms 4 ms 9 ms 10.188.8.37

5 3 ms 3 ms 2 ms 10.188.20.66



**【答**】：

（3）查看 ICMP echo 分组 ，是否这个分组和前面使用 ping 命令的ICMP echo 一样？若不一样，请分析使用tracert 命令后收到的分组里TTL 值的变化规律。

**【答**】：不一样，ping命令的ICMP echo的TTL值不变。ping命令：request的TTL值是148不变；而reply的TTL值是49不变； ICMP命令：request的TTL值是不断增长的，不过reply的TTL值是不变的为49，且只有目的主机发回reply包，中间路由器不发送reply包。

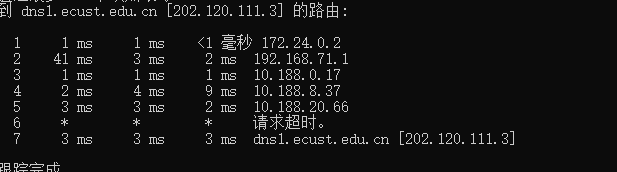
（4）对照 ICMP 协议，分析一下ICMP 超时报告分组比ICMP echo 分组多包含的信息有哪些？

**【答**】： IP数据报的首部以及TCP或UDP协议的端口号。

（5）对于ICMP超时报告分组，找出与命令提示窗口截图中的第六跳路由器的接口IP地址为多少？在wireshark抓包图中截图与第五跳路由器的接口IP地址对应的部分并截图。

**【答**】：

没有



**3. IP协议分析**

步骤1：分别在 PC1 和 PC2 上运行 wireshark，开始截获报文，为了只截获和实验内容有

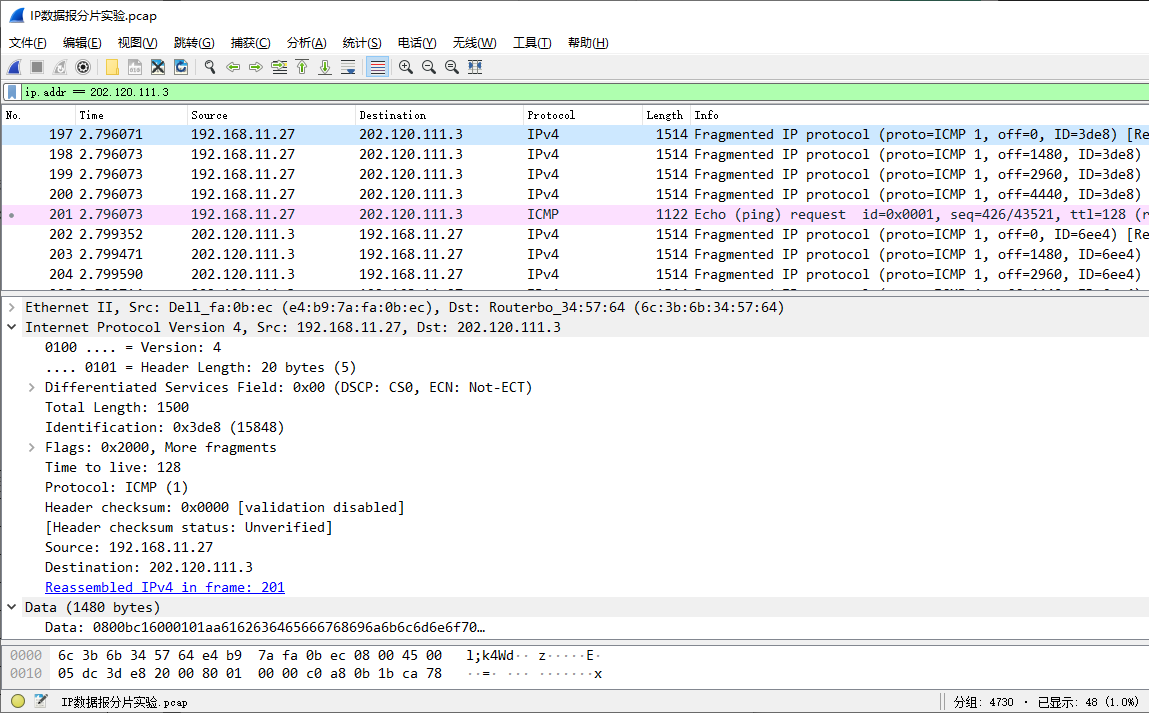
关的报文，将 wireshark 的 Captrue Filter 设置为“No Broadcast and no Multicast”；

步骤2： PC1 ping PC2；

步骤3：停止截获报文，分析截获的结果，回答下列问题：

（1）任取一个有 IP 协议的数据报并截图。

**【答**】：



（2）分析该 IP 协议的报文格式，完成下表。

表 IP 协议

|  |  |  |
| --- | --- | --- |
| **字段** | **报文信息** | **说明** |
| **版本** | 4 | IP协议的版本号位4 |
| **头长** | 20 bytes | IP协议包头部的长度 |
| **服务类型** | 0x00 (DSCP: CS0, ECN: Not-ECT) | 定义IP协议包的处理方法 |
| **总长度** | 1500 | IP包的总长度包括IP头和数据 |
| **标识** | 0x3de8 (15848) | 标识字段唯一地标识主机发送的每一份数据报 |
| **标志** | Flags: 0x2000, More fragments | 是一个3位的控制字段包含保留位、是否分片位、更多分片位 |
| **片偏移** | 0 | 定义该分片在原始分组中的偏移量 |
| **生存周期** | 128 | 表示数据包在网络上生存时间 |
| **协议** | ICMP (1) | 定义了IP数据报的数据部分使用的协议类型 |
| **校验和** | 0x0000 [validation disabled] | 是IPv4数据报包头的校验和 |
| **源地址** | 192.168.11.27 | 源站IP地址 |
| **目的地址** | 202.120.111.3 | 目的站IP地址 |

**4. IP数据报分片实验**

步骤1：在 PC1、PC2 两台计算机上运行 Wireshark，为了只截获和实验有关的数据报，设

置 Wireshark 的捕获条件为对方主机的 IP 地址的icmp协议；

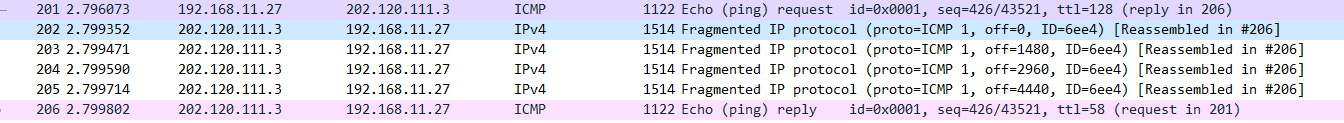
步骤2：在 PC1 上执行如下 Ping 命令，向主机 PC2 发送大小为7000个字节的数据报文；

步骤3：停止截获报文并回答下列问题：

（1）以太网的最大传输单元(MTU)是多少？怎么计算得出的？

**【答**】： 1500字节。从图中可观察到每一个分片所带的字节数为1480，又每个IP帧会在首部加上20个字节，所以MTU不超过1500字节

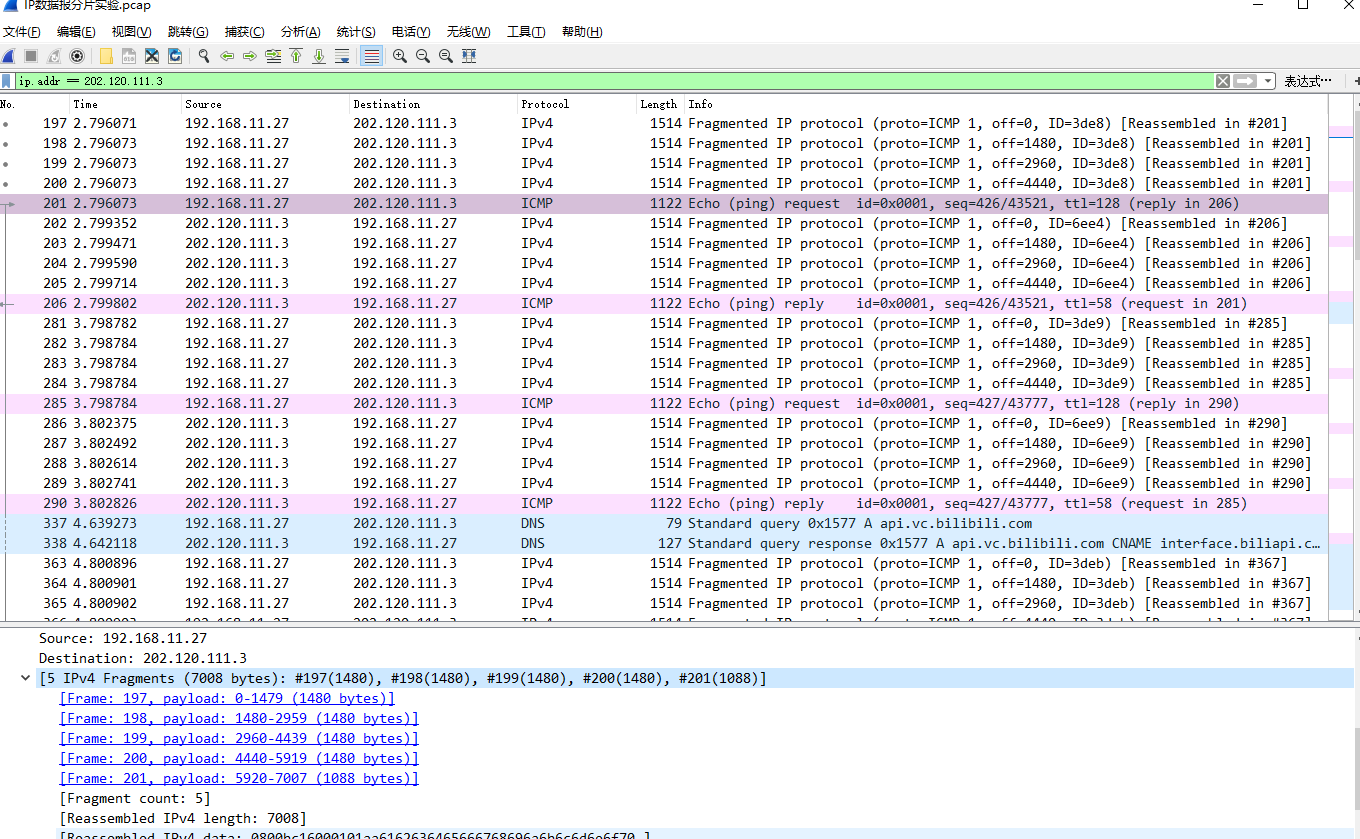
（2）分析截获的报文，将属于同 ICMP 请求报文的分片找出来并从wireshark 中截图，主机PC1 向主机 PC2 发送的 ICMP 请求报文分成了\_5个分片。



（3）ICMP 报文各分片的数据长度是多少？在wireshark 里截图显示。

**【答**】：

1500



（4）若要让主机PC1向主机PC2发送的数据分为2个分片，则 Ping 命令中的报文长度应为多大范围？为什么？

**【答】：**

因为MAC帧数据部分不能超过1500字节，同时，IP数据报会在ping命令报文长度上加20个字节作为IP数据报的首部，ICMP也会在整个报文的基础上加8字节。所以，假设ping命令报文长度为X,使得主机PC1向主机PC2发送的数据分为 2个分片。那么：

 𝑋+20+8>1500                                            ①

𝑋+20+20+8≤3000                                   ②

解①、②方程式，得      1472<X≤2952

所以，Ping命令中的报文长度应为[1473,2952]，且为整数。